

(19) World Intellectual Property Organization  
International Bureau(43) International Publication Date  
2 May 2002 (02.05.2002)

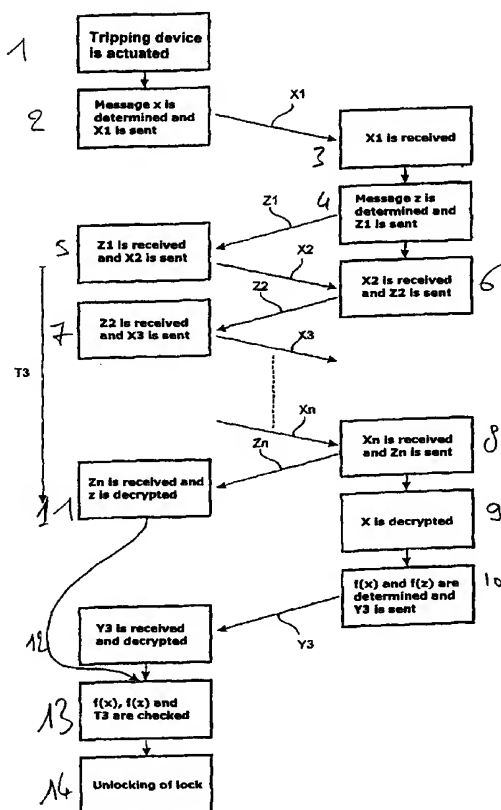
PCT

(10) International Publication Number  
**WO 02/35036 A1**

- (51) International Patent Classification<sup>7</sup>: **E05B 49/00** (74) Agent: **FRÖHLING, Werner**; Volvo Teknisk Utveckling AB, Corporate Patents, Dep. 06820, CTP, S-412 88 Göteborg (SE).
- (21) International Application Number: PCT/SE01/02321
- (22) International Filing Date: 23 October 2001 (23.10.2001) (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (25) Filing Language: Swedish
- (26) Publication Language: English
- (30) Priority Data:  
0003833-1 23 October 2000 (23.10.2000) SE
- (71) Applicant (*for all designated States except US*): **VOLVO TEKNISK UTVECKLING AB** [SE/SE]; S-405 08 Göteborg (SE).
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (72) Inventor; and
- (75) Inventor/Applicant (*for US only*): **LUNDKVIST, Ola** [SE/SE]; Nilssonsberg 10, S-411 43 Göteborg (SE).

[Continued on next page]

(54) Title: A METHOD FOR CONTROLLING AUTHORIZATION TO AN OBJECT AND A COMPUTER PROGRAM PRODUCT FOR THE AUTHORIZATION CONTROL



(57) Abstract: The invention relates to a method for controlling authorization for access to an object, in which a signal communication via electromagnetic waves is established between the object and a wireless portable unit when a tripping device on the object is actuated. The signal communication comprises at least one first signal (X1...Xn) that is sent from the object to the portable unit, and at least one second signal (Y3, Z1...Zn) that is sent from the portable unit to the object in response to said first signal(s). Said second signal(s) comprise sufficient information for verifying that the portable unit has an approved identity. The verification information is checked, a distance is measured between the object and the portable unit and the authorization is confirmed if both the checked verification information is approved and the measured distance is less than a predetermined value. For the distance measurement, a time (T3) is measured for the transmission of at least one of said first signals and at least one of said second signals with verification information.



**Published:**

— with international search report

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**A method for controlling authorization to an object and a computer program product for the authorization control**

FIELD OF THE INVENTION

5 The present invention relates to a method for controlling authorization for access to an object, in which a signal communication via electromagnetic waves is established between the object and a wireless portable unit when a tripping device on the object is actuated, the signal communication comprising at least one first signal that is sent from the object to the portable unit and at least one second signal that is sent from  
10 the portable unit to the object in response to said first signal(s), in which said second signal(s) comprise sufficient information for verifying that the portable unit has an approved identity, in which the verification information is checked, in which a distance is measured between the object and the portable unit and in which the authorization is confirmed if both the checked verification information is approved  
15 and the measured distance is less than a predetermined value. The predetermined value corresponds to a maximal permitted distance between the portable unit and the object.

In addition, the invention concerns a method for controlling authorization for access  
20 to an object according to the preamble to claims 8 and 11. The invention also concerns computer program products for such authorization control.

The invention will be described below for authorization control for a vehicle, such as a car or truck. This is a preferred, but in no way limiting, application of the invention.  
25 In such a case, the tripping device normally consists of a door handle on the vehicle.

More specifically, the field of the invention is aimed at a so-called passive access control, which means that the person who is authorized to access the object does not need actively to use any key or remote control in order to unlock the object's  
30 door. Instead, the authorization is checked automatically via the abovementioned signal communication using electromagnetic waves between the vehicle and the

wireless unit carried by the person, when the vehicle's door handle is actuated. The door is unlocked automatically in the event of approved authorization.

#### PRIOR ART

5 Patent US 5,723,911 relates to a device for controlling access to a motor vehicle. This control is designed to be carried out without the user needing to actuate any key. A distance detection device on a transceiver carried by the user is designed to detect the distance between the transceiver and the vehicle with the aim of reducing the risk of unauthorized access to the vehicle. The authorization control is carried  
10 out by a transmitter in the vehicle sending a call signal to a receiver in the transceiver when the vehicle's door handle is actuated. The transmitted signal has a short range. The transceiver's receiver receives the signal and sends a coded response signal back to the vehicle only if the vehicle is in the immediate vicinity of the transceiver. In other words, no response signal is sent back to the vehicle if this  
15 is not located in the vicinity of the transceiver. A receiving unit in the vehicle receives the response signal, checks it and sends an unlocking signal to the lock if the response signal is correct. The distance detection is carried out, for example, via transmission of a distance detection signal from the transceiver and reflection of this by the vehicle.

20

The distance detection is carried out as mentioned above with the aim of reducing the risk of unauthorized access to the vehicle. Such unauthorized access to the vehicle has previously been possible by the use of a pair of receiver-transmitters in the following way: a first person with a first transmitter-receiver is in the vicinity of the  
25 vehicle while a second person with a second transmitter-receiver stands in the vicinity of the authorized user of the vehicle. The first person actuates the door handle of the vehicle, which initiates the signal communication. The signal (with a short range) from the vehicle's transmitter is received by the first person's receiver and forwarded with a long range to the transmitter-receiver of the second person  
30 and thereafter to the rightful user of the vehicle. In the same way, the coded signal is thereafter sent back from the portable unit to the vehicle via the two pairs of transmitters-receivers and authorization is confirmed.

Using the distance detection device according to US 5,723,911, the time it takes for the electromagnetic waves or ultrasound waves to go from the portable unit to the object and back again is measured. If the rightful user is located at a great distance  
5 from the vehicle, the transmission of the ultrasound waves takes a long time. This is detected and a signal is not sent back to the vehicle from the portable unit.

A problem with said distance detection device is that it is not possible to know for certain that it is the correct (authorized) portable unit that is in the vicinity of the right  
10 vehicle. In addition, known methods for distance detection, such as ultrasound echoes and metal detection, are relatively easy to deceive and thereby not secure.

#### SUMMARY OF THE INVENTION

A first aim of the invention is to achieve a method for controlling authorization to an  
15 object with increased security in relation to previous technology.

This aim is achieved by measuring for the distance measurement a time for the transmission of at least one of said first signals and at least one of said second signals with verification information. In other words, the distance is determined  
20 between the object and the portable unit by measuring the time for at least part of the signal communication for the identity verification and it is ascertained that it really is the time between the correct portable unit and the object that has been measured. The signals for the identity control are thus used to determine whether the portable unit and the object are located sufficiently close to each other. This results in  
25 increased security.

Because the time is measured for the signals that are used for the identity control, the distance detection method that is separate to the identity control method according to previous technology is eliminated. In other words, according to the  
30 invention, the distance detection method is integrated in the identity control method.

An encryption system is suitably utilized for said signals. A strong encryption algorithm is preferably utilized. There are a plurality of known such encryption algorithms, and for example so-called asymmetric key pairs are used, with the object holding one key and the portable unit the other key. Simpler types of encryption or  
5 coding can also be used, which will of course not provide such high security.

According to a preferred embodiment, during the part of the signal communication that is used for the time measurement, a plurality of said signals are sent in series in such a way that alternate signals consist of one of said first signals and of one of  
10 said second signals. Because the time (and thereby any time deviation) for the consecutive signals, each of which has a very short transmission time, is totalled, it is thereby possible to determine with increased certainty whether the portable unit is located within the predetermined maximal permitted distance from the vehicle.

15 According to a second embodiment, at least one of said first signals comprises first information that is intended to be utilized for verifying the identity of the portable unit, in which the first information is processed by the unit and in which at least one of said second signal(s) with verification information comprises a first part with the first information in processed form. Said first verification information part in the  
20 lastmentioned second signal consists suitably of a function of the first information. By this means, increased security is obtained with regard to whether it is the correct portable unit that has received the first signal.

According to a further development of the previous embodiment, the lastmentioned  
25 second signal is sent after the conclusion of the time measurement. As the processing of the first information in the portable unit takes a certain, not always precisely foreseeable, time, the conditions are hereby created for a time measurement with high accuracy.

30 According to another embodiment, which is a further development of the previous embodiment, at least one of said second signals other than the lastmentioned signal comprises second verification information. To sum up, said first signal(s) thereby

comprise first verification information and said second signal(s), in addition to a suitably last of these in time, comprise second verification information. By utilizing these first and second signals for said time measurement, the conditions are created for achieving a time measurement with high accuracy. The contents in the first and the second verification information are suitably independent of each other.

According to a further development of the previous embodiment, the lastmentioned second signal comprises, in addition to the first verification information part, also a second part that comprises the second verification information in processed form. This results in increased security with regard to it being the correct portable unit that receives said first signals and sends said second signals.

A second aim of the invention is to achieve a specific method for the object for controlling authorization to the object with increased security in relation to previous technology.

This aim is achieved by a signal communication via electromagnetic waves being established between the object and a wireless portable unit when a tripping device arranged on the object is actuated, in which the signal communication comprises at least one first signal, that is sent from the object to the portable unit, and at least one second signal that is sent from the portable unit in response to said first signal(s) after the reception of the first signal and that is received by the object, in which said second signal(s) comprise sufficient information for verifying that the portable unit has approved identity, and in which the verification information is checked. In order to determine the distance between the object and the unit, a time is measured by the object from the transmission of one of said first signals until the reception of one of said second signals with verification information, the authorization is confirmed if both the checked verification information is approved and the measured time is less than a predetermined value.

A third aim of the invention is to achieve a specific method for a wireless portable unit for controlling authorization to an object with increased security in relation to previous technology.

5 This aim is achieved by a method intended to be used for controlling authorization for access to an object, in which at least one first signal, that was originally sent from the object via electromagnetic waves, is received by the portable unit, and in which a distance between the object and the portable unit is measured by the unit. At least one second signal is sent via electromagnetic waves from the portable unit to the  
10 object, in which said second signal(s) comprise sufficient information for verifying that the portable unit has approved identity, for the distance measurement, a time is measured from the transmission of one of said second signals with verification information until the reception of one of said first signals, which was sent after the reception of said second signal, and a result of the time measurement is sent to the  
15 object for confirmation of the authorization.

#### BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in greater detail in the following, with reference to the embodiments shown in the attached drawings.

20

Figure 1 shows schematically the object and the portable unit.

Figures 2-5 show in the form of block diagrams the signal communication between the object and the portable unit according to four embodiments of the invention.

25

#### DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Figure 1 shows schematically an authorization control device 15 comprising an object 1 and a wireless portable unit 2. The invention is described below in the case in which the object 1 consists of a vehicle. The wireless portable unit 2 is preferably  
30 sufficiently small to be carried in the user's pocket and is suitably the shape of a card or a flat object.



The vehicle 1 comprises a tripping device 3 in the form of a door handle. Both the vehicle 1 and the portable unit 2 comprise a transmitter 5, 50 and a receiver 6, 60 for signal communication via electromagnetic waves. Similarly, both the vehicle 1 and the portable unit 2 comprise a control unit 7, 70 for controlling the signal communication.

The control unit 7 of the vehicle 1 comprises a memory, which in turn comprises a program segment, or software components, for controlling at least part of the signal communication. The control unit 7 is arranged to check information transmitted by the portable unit 2 during the signal communication, to measure the signal time and to compare the measured signal time with a predetermined value for the purpose of determining whether the vehicle 1 and the user card 2 are located sufficiently near to each other during the signal communication. Similarly, the control unit 7 of the vehicle 1 is arranged to determine at least a part of the information in the signals that are to be sent from the vehicle for the identity information control.

The vehicle comprises a lock 11 connected to the control unit 7, which lock is suitably arranged for locking/unlocking the door of the vehicle to which the door handle 3 belongs.

The control unit 70 of the portable unit is arranged to determine at least a part of the information in the signals that are to be sent from the unit for the identity control, and to control identity information sent by the object 1.

The information in all signals with identity information that are sent between the vehicle 1 and the portable unit 2 is encrypted in such a way that the information in a message transmitted by the object can only be decrypted in its entirety by the portable unit 2 and vice versa. Such an encryption method is normally called strong encryption. A so-called asymmetric key pair is used for the decryption function, the control unit of the portable unit holding one of the keys and the control unit of the object holding the other key. The key of the portable unit 2 comprises identity information for the portable unit and the key of the vehicle 1 comprises identity

information for the vehicle. Alternatively, symmetric encryption can be used, which means that the vehicle and the portable unit have the same key.

The signal communication between the vehicle 1 and the portable unit 2 according to four preferred embodiments of the invention is described below with reference to Figures 2-5.

Figure 2 illustrates a first embodiment of the signalling method between the vehicle 1 and the portable unit 2.

Signal communication via electromagnetic waves is established between the vehicle 1 and the portable unit 2 when the door handle 3 is actuated. The control unit 7 of the object 1 then creates a message that comprises first information  $x$  that is intended to be utilized for verifying the identity of the portable unit. The first information  $x$  consists of identity information  $O\_ID$  unique to the object and a random number  $O\_RND$  generated by the control unit 7. The message is encrypted and sent to the portable unit 2 in a first signal  $X$ .

The portable unit 2 receives the first signal  $X$  and decrypts the message. The portable unit 2 processes the first information  $x$  and sends a second encrypted signal  $Y1$  to the object 1. The second signal  $Y1$  comprises the first information  $x$  in processed form, more specifically a function  $f(x)$  of the first information  $x$ . In particular,  $f(x)$  comprises the message part  $E\_SVAR = f(O\_RND)$ . The signal  $Y1$  is received by the object 1 and the message is decrypted. A time  $T1$  is measured by the control unit 7 of the object 1 from the transmission of the first signal  $X$  until the reception of the second signal  $Y1$ .  $E\_SVAR$  and  $T1$  are checked by the object 1, after which the lock 11 is unlocked if  $E\_SVAR = f(O\_RND)$  and the measured time is less than a predetermined value.

Figure 3 illustrates a second embodiment of the signalling method between the vehicle 1 and the portable unit 2, which is a further development of the first embodiment.

According to this second embodiment, two second signals Z, Y2, are sent from the portable unit 2 to the object 1 in response to the signal X. A first Z of these second encrypted signals comprises second verification information z. The control unit 70  
5 creates namely a message that consists of identity information E\_ID that is unique to the unit 2 and a random number E\_RND. The second signal Y2 that is last in time comprises a first part f(x), as described above, and a second part f(z). In particular, f(z) comprises the message part E\_VER = f(E\_RND). A time T2 is measured by the control unit 7 of the object 1 from the transmission of the first signal X until the  
10 reception of the first in time Z of said second signals. When Y2 has been received and decrypted, f(x) (=E\_SVAR), f(z) (=E\_VER) and T2 are checked, after which the lock 11 is unlocked if E\_SVAR = f(O\_RND), E\_VER = f(E\_RND) and the measured time is less than a predetermined value.

15 The processing of said first and second information (x and z respectively) is here carried out after the time measurement has been completed. Using a suitable signalling algorithm, the requisite time from the reception of the first signal X until the transmission of the second signal Z can be predicted with high accuracy. For this, a signalling algorithm that is highly time-deterministic is required.

20 Figure 4 illustrates a third embodiment of the signalling method between the vehicle 1 and the portable unit 2, which is a further development of the second embodiment.

A plurality of first signals  $X_i$  are sent from the object 1 to the portable unit 2 and a  
25 plurality of second signals  $Z_i$ , Y3 are sent from the portable unit 2 to the object 1. The first information x described above is encrypted and the result is divided up into a plurality of parts, which are sent in said first signals  $X_i$ . The second information z described above is encrypted and the result is divided up in the same way into a plurality of parts, which are sent in said second signals  $Z_i$ . The signals  $X_2..X_n$  and  
30  $Z_1..Z_n$  are sent in series and in such a way that every second signal consists of one of said first signals and every second signal consists of one of said second signals. A time T3 is measured by the control unit 7 of the object 1 from the transmission of

the second in time  $X_2$  of said first signals until the reception of the last second signal  $Z_n$  with the second verification information. When all the signals  $X_2-X_n$  and  $Z_1-Z_n$  have been received, the information  $x$  and  $z$  respectively can be obtained.

- 5 The last in time second signal  $Y_3$  is thereafter produced in the same way as the above described  $Y_2$ .

As an alternative to the first information  $x$  being first encrypted and the result thereafter being divided up, the information can first be divided up into said plurality  
10 of parts, after which each of the parts is encrypted. In the same way, the second information can, of course, first be divided up into said plurality of parts, after which each of the parts is encrypted.

The components of the portable unit 2 used for the signal communication are, for  
15 example, arranged in a passive state until the tripping device 3 is actuated. When the receiver of the portable unit receives the signal  $X_1$  from the object following said actuation of the tripping device, said components change to an active state. The content  $z$  in the second signals from the portable unit 2 used for the time measurement is now determined. Thereafter the second signal  $Z_1$  is sent back to  
20 the object. Because the time is measured from the transmission of the second in time  $X_2$  of said first signals, the changeover from passive state to active state is not included in the time measurement. This means that the time measurement is carried out during a part of the signal communication, the time from the reception of a signal until the transmission of a subsequent signal in both the object and the portable unit  
25 being able to be predicted with high accuracy.

The total time for the part of the signal transmission that is utilized for the time measurement can thereby also largely be predicted. By this means, good conditions are created for eliminating the risk that the attempted unauthorized access to the  
30 vehicle described above will succeed.

As the signals are sent in series, any time deviation that occurs for the signal time forward and backward between the vehicle and the portable unit is totalled. Such a time deviation corresponds to the portable unit, and hence the user, being located at a distance greater than a maximal permitted distance from the vehicle. Because of  
5 said totalling, it is possible to determine more reliably whether the owner of the portable unit is located in the vicinity of the vehicle. The more signals that are used for the time measurement, the more secure the method. The number of signals from the unit that are included in the time measurement is at least one, preferably at least two, suitably at least 10 and in particular at least 100. The number of signals that is  
10 used depends on how high security is desired/required for the authorization control.

The whole message, and hence the content in each of the signals  $X_i$ , from the vehicle is determined when the tripping device is actuated. In a corresponding way, the whole message, and hence the content in each of the signals  $Z_i$ , from the unit is  
15 determined when the unit receives the first signal  $X$  from the vehicle. By this means, the signalling method during the subsequent time measurement, that is the reception of a signal and transmission of the next signal from both the vehicle and the unit, will only consist of a number of well-defined operations. The time required for this method can thereby be predicted with high accuracy.

20

When the control unit 70 of the portable unit 2 has sent the last signal with said identity information part to the vehicle, it decrypts the total message from the vehicle using its encryption key. The decrypted message  $x$  has two parts, namely  $O\_ID$  and  $O\_RND$ . The portable unit 2 thereafter sends the last signal  $Y3$  to the vehicle with  
25 information that it has received the whole message and succeeded in decrypting it, which is verified by the number  $O\_RND$  being included in the signal. More specifically, the message part is created  $E\_SVAR = f(O\_RND)$ . The last signal  $Y3$  from the portable unit also comprises the message part  $E\_RND$ . More specifically,  $E\_VER = f(E\_RND)$  is created for the lastmentioned message part.

30

When the control unit 7 of the vehicle 1 has received for the time measurement the last  $Z_n$  of said second signals with said identity information part from the portable

unit 2, it decrypts the message using its encryption key. The decrypted message  $f(z)$  has two parts, namely  $E\_ID$  and  $E\_RND$ . Authorization is confirmed after the control unit 7 of the vehicle 1 has received the last signal  $Y3$  from the portable unit 2, provided that:

- $E\_ID$  is an approved key,
- $E\_SVAR = f(O\_RND)$ ,
- $E\_VER = f(E\_RND)$ , and
- the measured time is less than or equal to a predetermined value that corresponds to a maximal permitted distance between the portable unit and the object.

Figure 5 illustrates a fourth embodiment of the signalling method between the vehicle 1 and the portable unit 2, which is a variant of the third embodiment and differs from this in that a signal transmission time  $T4$  is measured by the control unit 70 of the unit 2. A signal  $Y4$  also comprises a result of this time measurement, in addition to the information in said signal  $Y3$ .

Both the control unit 7 of the object 1 and the control unit 70 of the portable unit 2 comprise a memory, which in turn comprises a computer program product with program segments or a program code, for carrying out all the steps according to any one of the embodiments described above when the program is executed. The computer program product can be transmitted to the object or the portable unit in various ways via a propagating signal, for example via downloading from another computer, via cable and/or wireless means, or by the installation of a memory circuit. In particular, the propagating signal can be transmitted via the Internet. The term computer unit used in the claims refers to said control unit.

When the authorization is confirmed, an unlocking signal is sent from the vehicle's control unit to a lock on a door of the vehicle, which is thereby unlocked automatically.

The predetermined time value that corresponds to a maximal permitted distance between the portable unit and the object depends, of course, on the number of signals that are included in the time measurement.

- 5 The embodiments described are only to be regarded as preferred examples and a number of further variants and modifications are possible within the scope of the following claims. For example, the portable unit can be programmed to determine the information in the message in its entirety before it receives the first signal from the object.

10

The invention is in particular intended for electromagnetic waves in the form of radio waves or microwaves. The frequency range or frequency ranges of the waves are preferably selected within a range where they are not subject to inference from other strong signals.

15

It is, of course, within the scope of the following claims to send signals without identity information between, before and/or after the signals with the identity information during the time measurement.

- 20 The number of signals that are to be sent from the portable unit for the identity control and/or the time measurement can, of course, be determined by the control unit 70.

It is, of course, also possible to vary the content in the signals used for the transmission of the identity information, while remaining within the scope of the claims.

25 The invention described above is, of course, not limited in any way to application to a vehicle, but could, for example, be used for controlling authorization for access to a stationary object, such as a building, a room or part of a building. The invention is similarly applicable to factory premises or an enclosed area, for example bounded by a fence, railings or the like. Nor is the invention restricted to the unlocking of a

30

previously locked lock, but could of course also be used for locking a previously unlocked lock.

5 In addition, instead of a door handle, the tripping device 3 can also consist of an optical sensor, a sensor that detects heat, movement or pressure, radar or other type of sensor.



## CLAIMS

1. A method for controlling authorization for access to an object (1), in which a signal communication via electromagnetic waves is established between the object and a wireless portable unit (2) when a tripping device (3) on the object is actuated, the signal communication comprising at least one first signal (X, X1..Xn), that is sent from the object to the portable unit, and at least one second signal (Y1, Y2, Y3, Y4, Z1..Zn), that is sent from the portable unit to the object in response to said first signal(s), in which said second signal(s) comprise sufficient information for verifying that the portable unit has an approved identity, in which the verification information is checked, in which a distance is measured between the object and the portable unit, and in which the authorization is confirmed if both the checked verification information is approved and the measured distance is less than a predetermined value,
- characterized in that for the distance measurement, a time (T1, T2, T3, T4) is measured for the transmission of at least one of said first signals and at least one of said second signals with verification information.
2. A method according to claim 1, characterized in that during the part of the signal communication that is used for the time measurement, a plurality of said signals (X2..Xn, Z2..Zn) are sent in series in such a way that alternate signals consist of one of said first signals (X2..Xn) and of one of said second signals (Z2..Zn).
3. A method according to claim 1 or 2, characterized in that at least one of said first signals (X, X1..Xn) comprises first information that is intended to be utilized for verifying the identity of the portable unit (2), in that the first information is processed by the unit and in that at least one of said second signal(s)

(Y1, Y2, Y3, Y4) with verification information comprises a first part with the first information in processed form.

4. A method according to claim 3, characterized in that the lastmentioned  
5 second signal (Y1, Y2, Y3, Y4) is sent after the conclusion of the time measurement.

5. A method according to claim 3 or 4,  
characterized in that  
at least one (Z1..Zn) of said second signals other than the lastmentioned signal (Y1,  
10 Y2, Y3, Y4) comprises second verification information.

6. A method according to claim 5, characterized in that the second signal (Y1,  
Y2, Y3, Y4) with the first verification information part also comprises a second part  
that comprises the second verification information in processed form.

15

7. A method according to claim 3, 4 or 6,  
characterized in that the portable unit (2) checks said first information transmitted  
from the object in said first signal(s) (X1..Xn), and in that it sends the second signal  
(Y1, Y2, Y3, Y4) with said verification part(s) only if the checked information is  
20 approved.

8. A method for controlling authorization for access to an object (1), in which a  
signal communication via electromagnetic waves is established between the object  
and a wireless portable unit (2) when a tripping device (3) on the object is actuated,  
25 the signal communication comprising at least one first signal (X, X1..Xn), that is sent  
from the object to the portable unit, and at least one second signal (Y1, Y2, Y3,  
Z1..Zn), that is sent from the portable unit in response to said first signal(s) after the  
reception of the first signal and is received by the object, in which said second  
signal(s) comprise sufficient information for verifying that the portable unit has an  
30 approved identity, and in which the verification information is checked,  
characterized in that

for determining the distance between the object and the unit, a time (T1, T2, T3) is measured by the object from the transmission of one of said first signals until the reception of one of said second signals with verification information, and in that the authorization is confirmed if both the checked verification information is approved  
5 and the measured time is less than a predetermined value.

9. A method according to claim 8, characterized in that during the part of the signal communication that is used for the time measurement, a plurality of said first signals (X, X1..Xn) are sent, and at least during a section of the  
10 time measurement, each of these is sent after one of said second signals (Z1..Z3) has been received.

10. A method according to claim 8 or 9, characterized in that

15 at least one of said first signals (X, X1..Xn) comprises first information that is intended to be processed by the portable unit (2) and to be utilized for verifying the identity of the portable unit.

11. A method intended to be used for controlling authorization for access to an  
20 object (1), in which at least one first signal (X, X1..Xn), that was originally sent from the object (1), via electromagnetic waves, is received by the portable unit, and in which a distance between the object and the portable unit is measured by the unit, characterized in that

at least one second signal (Y4, Z1..Zn) is sent via electromagnetic waves from the  
25 portable unit (2) to the object (1), in which said second signal(s) comprise sufficient information for verifying that the portable unit has approved identity, in that for the distance measurement, a time (T4) is measured from the transmission of one of said second signals with verification information until the reception of one of said first signals, which was sent after the reception of said second signal, and in that a result  
30 of the time measurement is sent to the object for confirmation of the authorization.

12. A method according to claim 11, characterized in that

during the part of the signal communication that is used for the time measurement, a plurality of said second signals ( $Z2..Zn$ ) are sent and each of these is sent after one of said first signals ( $X2..Xn$ ) has been received.

5 13. A method according to claim 11 or 12,  
characterized in that  
first information that is intended to be utilized for verifying the identity of the portable  
unit (2) and that is included in at least one of said first signals ( $X, X1..Xn$ ) is  
processed by the unit, and in that one of said second signal(s) ( $Y4$ ) with verification  
10 information comprises a first part with the first information in processed form.

14. A method according to claim 13, characterized in that the lastmentioned  
second signal ( $Y4$ ) is sent after the conclusion of the time measurement.

15 15. A method according to claim 13 or 14,  
characterized in that  
at least one ( $Z1..Zn$ ) of said second signals other than the lastmentioned signal ( $Y4$ )  
comprises second verification information.

20 16. A method according to claim 15, characterized in that  
the second signal ( $Y4$ ) with the first verification information also comprises a second  
part that comprises the second verification information in processed form.

17. A method according to claim 13, 14 or 16,  
25 characterized in that the portable unit (2) checks said first information transmitted  
from the object (1) in said first signal(s) ( $X, X1..Xn$ ), and in that it sends the second  
signal with said verification part(s) only if the checked information is approved.

18. A method according to any one of claims 1-17,  
30 characterized in that  
the content in the signals intended for the time measurement is determined before  
the commencement of the time measurement.

19. A method according to any one of claims 1-18,  
characterized in that  
a lock (11) on the object (1) is locked/unlocked in the event of authorization being  
5 confirmed.

20. A method according to any one of claims 1-19,  
characterized in that  
the object consists of a vehicle.

10

21. A method according to any one of claims 1-20,  
characterized in that  
the tripping device (3) consists of a door handle on a vehicle.

15 22. A computer program product comprising program segments for causing a  
computer unit in the object (1) to carry out the steps according to any one of Claims  
8-10.

20 23. A computer program product comprising program segments for causing a  
computer unit in the wireless portable unit (2) to carry out the steps according to any  
one of Claims 11-17.

1/5

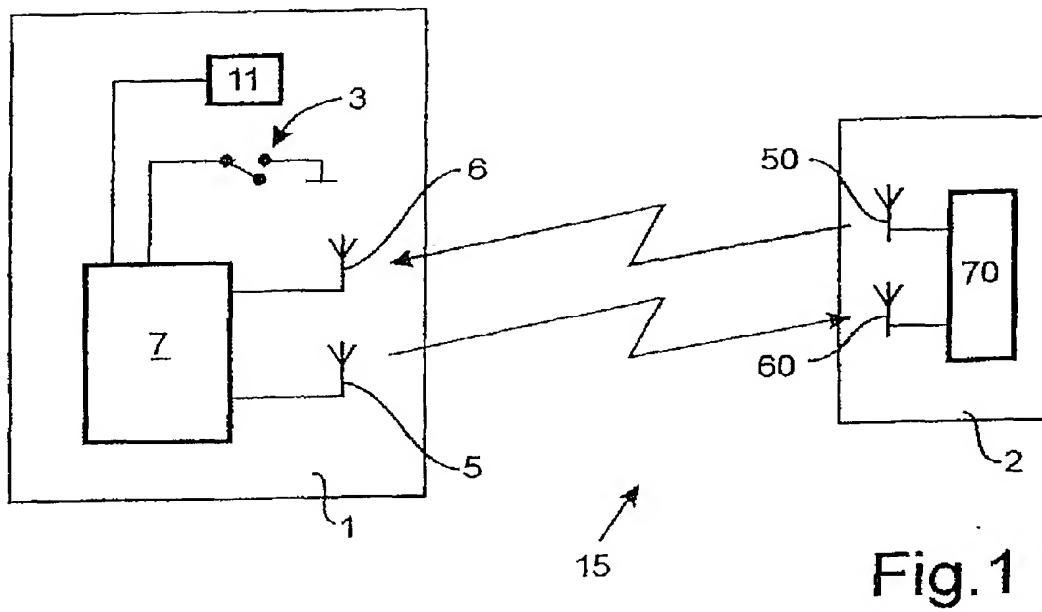


Fig.1

2/5

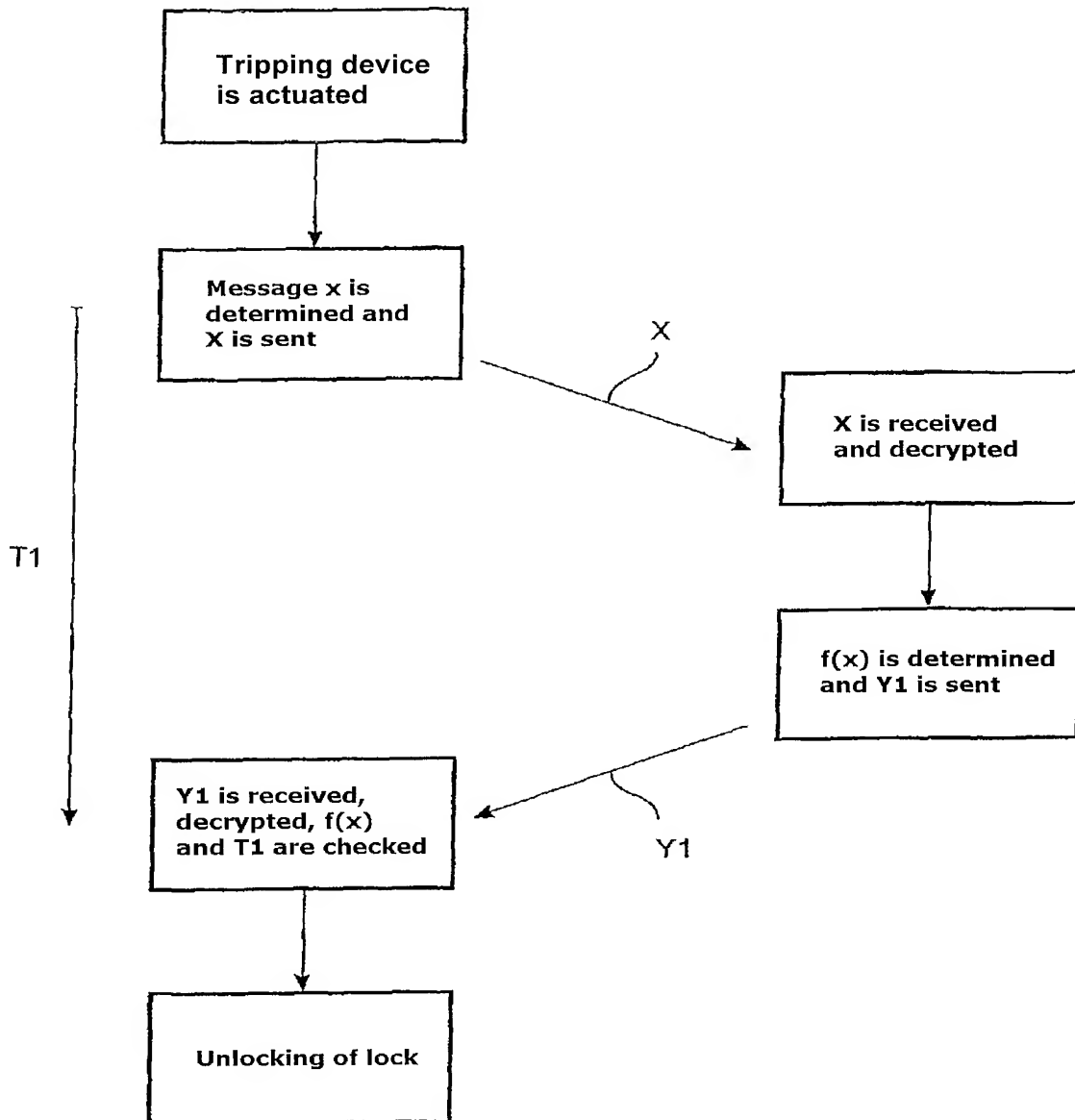


Fig.2

3/5

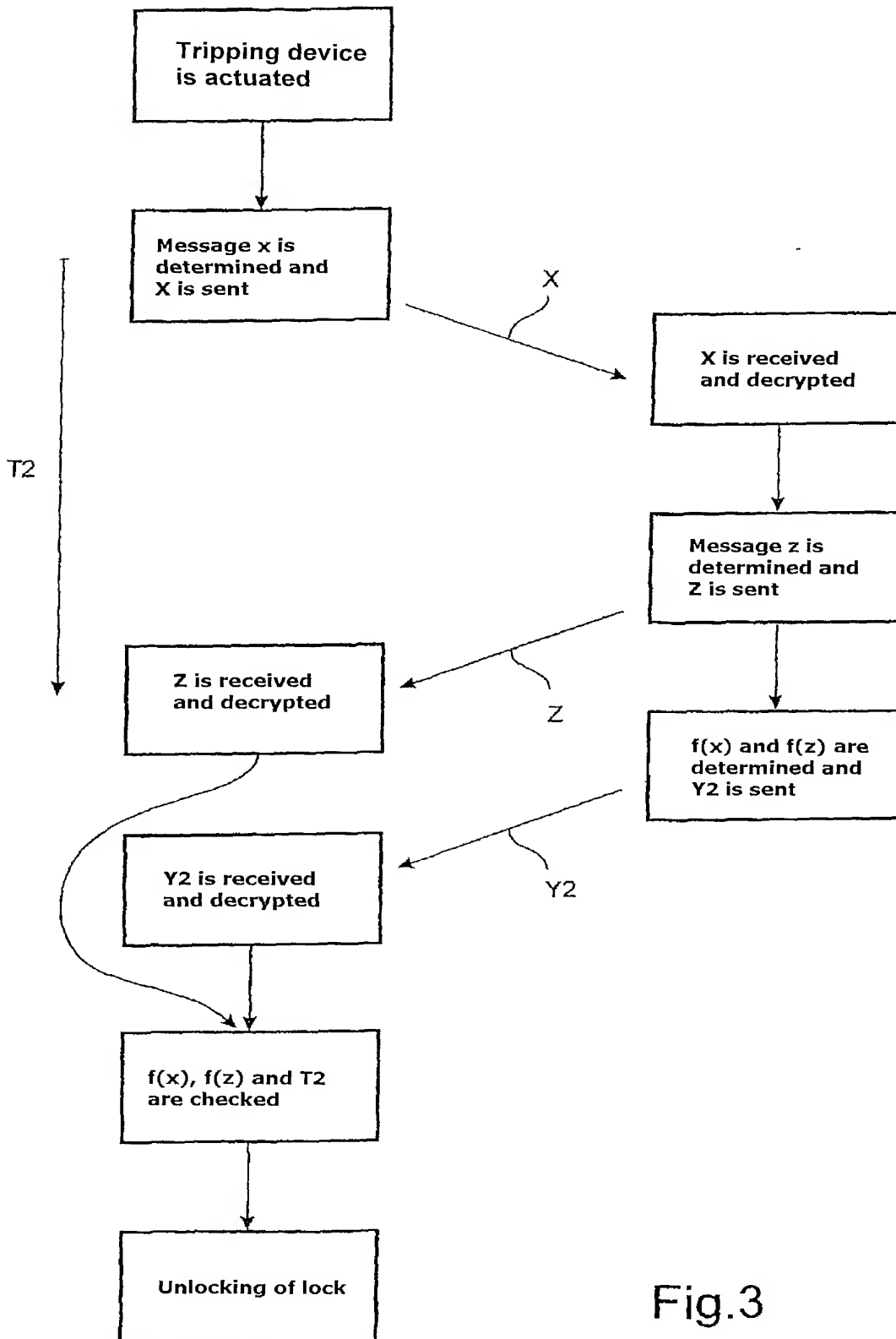


Fig.3



4/5

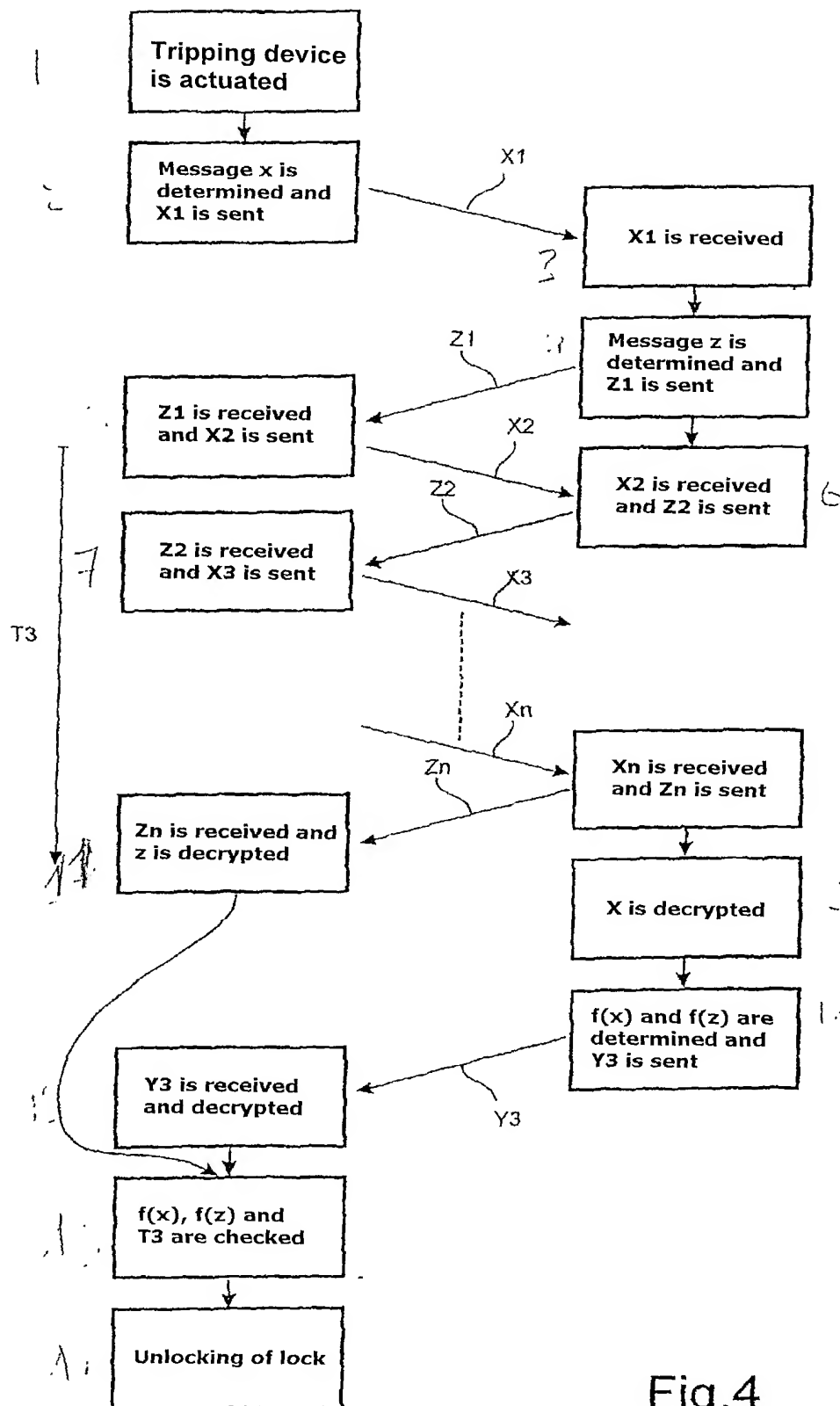


Fig.4

~~X~~

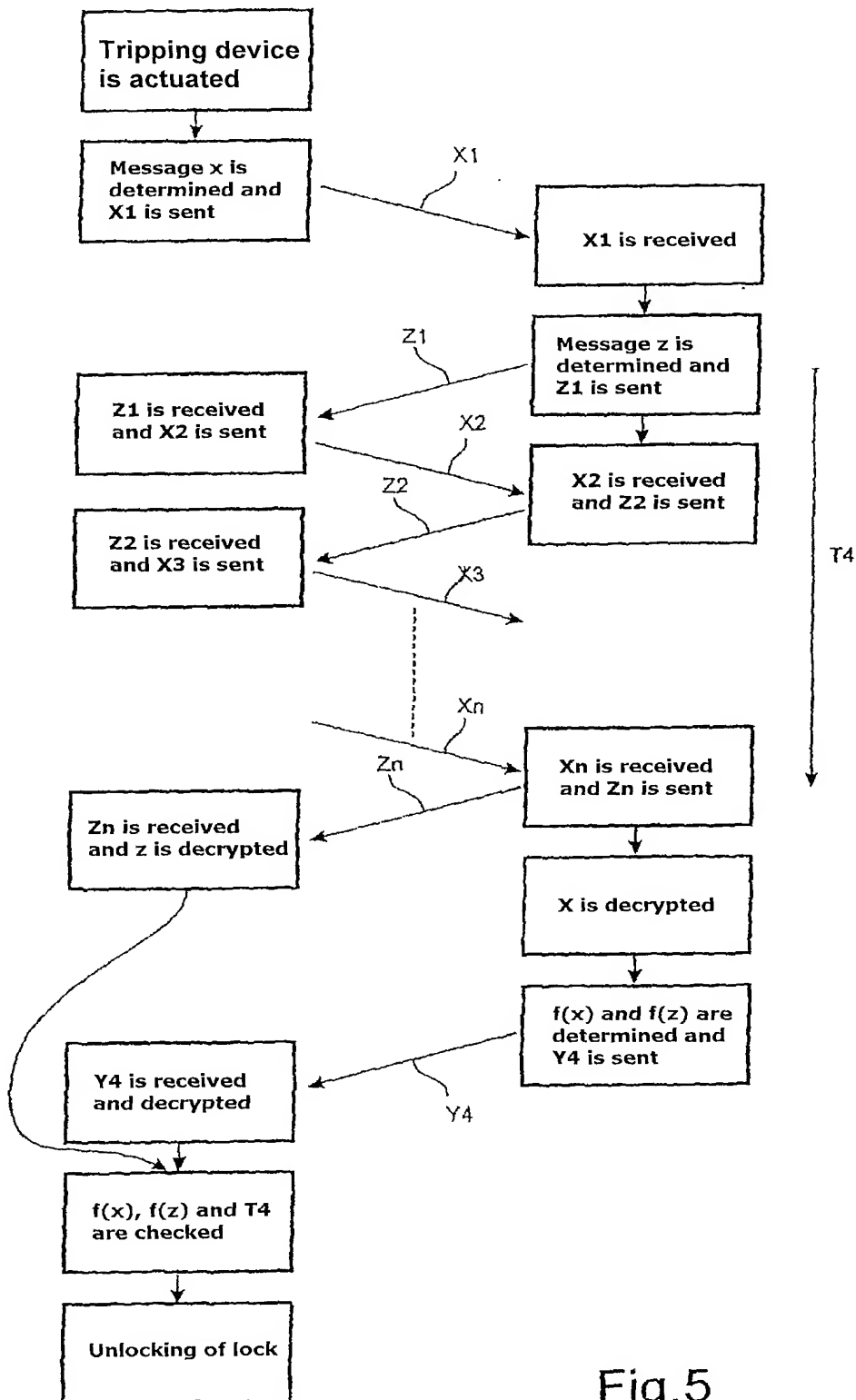


Fig.5

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 01/02321

## A. CLASSIFICATION OF SUBJECT MATTER

IPC7: E05B 49/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 19846803 C1 (DAIMLERCHRYSLER AG), 7 Sept 2000 (07.09.00)	1,8
Y	--	2-7,9-23
X	WO 0012848 A1 (LEOPOLD KOSTAL GMBH & CO. KG), 9 March 2000 (09.03.00)	1,8
Y	--	2-7,9-23
X	DE 19854128 A1 (MANNESMANN VDO AG), 31 May 2000 (31.05.00)	1,8
Y	--	2-7,9-23

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

30 January 2002

Date of mailing of the international search report

07-02-2002

Name and mailing address of the ISA

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Christer Wendenius / MRo

Telephone No. +46 8 782 25 00

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 01/02321

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5723011 A (M. GLEHR), 3 March 1998 (03.03.98) --	11-21,23
Y	US 4596985 A (W. BONGARD ET AL), 24 June 1986 (24.06.86) --	2-20
Y	US 3503680 A (S. SCHENKERMANN), 31 March 1970 (31.03.70) --	2-20
A	DE 4306819 A1 (MITSUBISHI DENKI K.K.), 9 Sept 1993 (09.09.93) --	
A	WO 9967486 A1 (BAYERISCHE MOTOREN WERKE AKTIENGESELLSCHAFT), 29 December 1999 (29.12.99) --	
A	DE 19832203 A1 (LEOPOLD KOSTAL GMBH & CO KG), 20 January 2000 (20.01.00) --	
A	DE 4440855 A1 (SIMONS, O. ET AL), 30 May 1996 (30.05.96) --	
A	EP 0773148 A1 (VOLKSWAGEN AKTIENGESELLSCHAFT), 14 May 1997 (14.05.97) -- -----	

## INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/02

International application No.

PCT/SE 01/02321

Patent document cited in search report			Publication date	Patent family member(s)	Publication date
DE	19846803	C1	07/09/00	EP 0992408 A US 6208239 B	12/04/00 27/03/01
WO	0012848	A1	09/03/00	AU 5737299 A BR 9913440 A DE 19839696 A,C EP 1109981 A DE 19839695 C DE 19926234 A	21/03/00 02/10/01 02/03/00 27/06/01 04/05/00 14/12/00
DE	19854128	A1	31/05/00	EP 1004726 A	31/05/00
US	5723011	A	03/03/98	NONE	
US	4596985	A	24/06/86	DE 3244049 A,C FR 2536781 A,B GB 2131992 A,B GB 8331329 D IT 1167020 B IT 8323862 D JP 1763520 C JP 4051626 B JP 59206573 A SE 466510 B,C SE 8306489 A SE 8903745 A	20/09/84 01/06/84 27/06/84 00/00/00 06/05/87 00/00/00 28/05/93 19/08/92 22/11/84 24/02/92 28/05/84 09/05/91
US	3503680	A	31/03/70	NONE	
DE	4306819	A1	09/09/93	FR 2689264 A,B JP 2821306 B JP 5250326 A US 5355413 A	01/10/93 05/11/98 28/09/93 11/10/94
WO	9967486	A1	29/12/99	DE 19827722 A EP 1090199 A	23/12/99 11/04/01
DE	19832203	A1	20/01/00	WO 0004517 A	27/01/00
DE	4440855	A1	30/05/96	NONE	
EP	0773148	A1	14/05/97	NONE	